REMARKS

Claims 1-20 are currently pending in the application. By this response, no claims are amended, added, or canceled. Reconsideration of the rejected claims in view of the following remarks is respectfully requested.

35 U.S.C. §102 Rejection

Claims 1-20 are rejected under 35 U.S.C. §102(b) as being anticipated by U.S. Pat. Pub. No. 2003/0028803 issued to Bunker, V et al. ("Bunker"). This rejection is respectfully traversed.

A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). See MPEP §2131. Applicants submit that the applied art does not show each and every feature of the claimed invention.

As discussed in Applicants' previous response, this invention relates in general to network security, and more particularly to a method for providing network perimeter security assessment. As opposed to prior art systems in which any given security tool is specific to a single discipline, embodiments of the invention provide a comprehensive network perimeter security assessment. By providing a method for checking network perimeter security that incorporates more than one network security discipline, an enterprise architecture that is more secure from attacks to computers and network devices may be developed. More specifically, independent claims 1, 16, and 18 each recite plural (e.g., four) reviewing steps and generating a report concerning security of the perimeter based upon all of the reviewing steps. More specifically, representative independent claim 1 recites:

> ...reviewing security of a network perimeter architecture;
> reviewing security of data processing devices that transfer data across the perimeter of the network;
> reviewing security of applications that transfer data across said perimeter;
> reviewing vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter; and
> generating a report concerning security of said perimeter based upon all of the reviewing steps.

Thus, the independent claims each recite performing four reviews: (i) a network perimeter architecture review; (ii) a device review; (iii) an applications review; and (iv) a vulnerability of devices and applications review. By generating a report based upon all four of the reviewing steps, the claimed invention provides a comprehensive method for checking network perimeter security.

The Examiner asserts that Bunker discloses all of the features of independent claim 1 at paragraphs 0010 and 0012 (Final Office Action, pages 2-3). Also, the Examiner groups the rejection of independent claims 16 and 18 with that of claim 1 (Final Office Action, page 21). Applicants respectfully disagree with the rejection, and submit that Bunker does not disclose performing (i) a network perimeter architecture review, (ii) a device review, or (iii) an applications review. Moreover, as Bunker does not disclose these reviews, Applicants submit that Bunker cannot reasonably be said to disclose generating a report based upon (i) a network perimeter architecture review; (ii) a device review; (iii) an applications review; and (iv) a vulnerability of devices and applications review, as recited in the claimed invention.

As indicated in Bunker's title, and at numerous instances throughout the specification, Bunker discloses a network vulnerability assessment system and method. That is, Bunker discloses a methodology for determining the vulnerability of a customer system by launching

numerous basic tests that simulate hackers attempting to harm the customer system. This is demonstrated by the following passages of Bunker:

> [0010] ... The preferred embodiment provides real-time network security vulnerability assessment tests, possibly complete with recommended security solutions. External vulnerability assessment tests may emulate hacker methodology in a safe way and enable study of a network for security openings, thereby gaining a true view of risk level without affecting customer operations. This assessment may be performed over the Internet for domestic and worldwide corporations.
>
> ...
>
> [0069] Figuratively, the Command Engine 116 is the "brain" that orchestrates all of the "basic tests" 516 into the security vulnerability attack simulation used to test the security of customer systems and networks 1002. While the Command Engine 116 essentially mimics hackers, the tests 516 themselves should be harmless to the customer. Each basic test 516 may be a minute piece of the entire test that can be launched independently of any other basic test 516. The attack simulation may be conducted in waves, with each wave of basic tests 516 gathering increasingly fine-grained information.
>
> ...
>
> [0094] The Testers 502 house the arsenals of tools 514 that can conduct hundreds of thousands of hacker and security tests 516. The Tester 502 may receive encrypted basic test instructions from the Gateway 118, via the Internet. The instructions inform the Tester 502 which test 516 to run, how to run it, what to collect from the customer system, etc. Every basic test 516 may be an autonomous entity that may be responsible for only one piece of the entire test that may be conducted by multiple Testers 502 in multiple waves from multiple locations. Each Tester 502 can have many basic tests 516 in operation simultaneously. The information collected by each test 516 about the customer systems 1002 may be sent to the Gateway 118.

As such, Bunker discloses performing a multi-wave vulnerability test. However, Bunker makes no mention of: (i) reviewing security of a network perimeter architecture; (ii) reviewing security of data processing devices that transfer data across the perimeter of the network; or (iii) reviewing security of applications that transfer data across said perimeter, as recited in the

claimed invention. Instead, Bunker only discloses vulnerability testing. Bunker does not disclose the other three types of security reviews recited in the claimed invention.

Moreover, because Bunker does not disclose the other three types of security reviews recited in the independent claims, it is arguably impossible for Bunker to disclose generating a report concerning security of said perimeter based upon all of the reviewing steps, as further recited in the claimed invention. Therefore, Bunker fails to disclose each and every feature of the claims, and does not anticipate the claimed invention.

Applicants submit that claims 2-15, 17, 19 and 20 depend from allowable independent claims, and are allowable based upon the allowability of the respective independent claims. Moreover, Bunker fails to disclose or suggest many of the features of the dependent claims.

For example, Bunker does not disclose that the reviewing security of data processing devices that transfer data across the perimeter of the network comprises categorizing components as either control points or non-control points, as recited in claim 12. The Examiner contends that Bunker discloses these features at paragraph 0073 (Final Office Action, page 18). Applicants respectfully disagree. The passage identified by the Examiner is totally silent as to categorizing devices that transfer data across the perimeter of the network. much less as to categorizing such devices as control points or non-control points. Instead, at paragraph 0073, Bunker describes determining which basic tests 516 to run, and assigning the tests 516 to a Tester 502. Bunker simply does not disclose categorizing devices as control points or non-control points in this, or any other, passage.

Furthermore, Bunker does not disclose: performing a policy review of an enterprise which owns or controls said network; defining review parameters based upon the policy review; and utilizing the review parameters to perform each of the four reviews recited in the

independent claim, as recited in claim 14. The Examiner asserts that Bunker discloses these features at paragraphs 0010-0012, 0059, 0149, and 0054. Applicants respectfully disagree. The passages referred to by the Examiner describe the multi-part vulnerability test. However, these passages do not disclose using parameters determined in a policy review in each of (i) a network perimeter architecture review, (ii) a device review, or (iii) an applications review. That is, Bunker does not disclose performing a first review (e.g., a policy review) to define parameters, then using those parameters in four other types of reviews (e.g., (i) a network perimeter architecture review, (ii) a device review, (iii) an applications review, and (iv) a vulnerability review).

Claims 17 and 20 recite that each of the four reviews utilize review parameters defined in a policy review of an enterprise which owns or controls said network. As discussed above with respect to claim 14, Bunker does not disclose performing a first review (e.g., a policy review) to define parameters, then using those parameters in four other types of reviews (e.g., (i) a network perimeter architecture review, (ii) a device review, (iii) an applications review, and (iv) a vulnerability review). Instead, Bunker only discloses a multi-wave vulnerability attack, wherein each wave is adjusted based upon data determined in the previous wave. However, such a vulnerability attack simply does not address the other types of review: (i) a network perimeter architecture review, (ii) a device review, or (iii) an applications review. Therefore, Bunker cannot be said to disclose that each of the four reviews utilize review parameters defined in a policy review of an enterprise which owns or controls said network, as recited in claims 17 and 20.

Accordingly, Applicants respectfully request that the §102 rejection of claims 1-20 be withdrawn.

Other Matters

Applicants note that the explanation of the rejection includes references to paragraph numbers and block quotations of text of Bunker. However, with multiple features recited in the claims, such general explanations of the complex Bunker document leave Applicants unsure of exactly what portions of Bunker are being applied to the respective features of the claims. For example, with respect to claim 1, the Examiner merely refers to paragraphs 0010 and 0012 of Bunker, and provides a block quote from those paragraphs. However, from this, it is unclear what element(s) of Bunker the Examiner considers as constituting reviewing security of a network perimeter architecture. Similarly, it is unclear what element(s) of Bunker the Examiner considers as constituting reviewing security of data processing devices that transfer data across the perimeter of the network, reviewing security of applications that transfer data across said perimeter, etc.

Applicants note 37 C.F.R. §1.104(c)(2) states that with regard to an Examiner's rejection of claims:

> In rejecting claims for want of novelty or for obviousness, the examiner must cite the best references at his or her command. When a reference is complex or shows or describes inventions other than that claimed by the applicant, the particular part relied on must be designated as nearly as practicable. The pertinence of each reference, if not apparent, must be clearly explained and each rejected claim specified. (emphasis added).

Additionally, the Examiner is reminded of the guidance provided by MPEP §707.07(f):

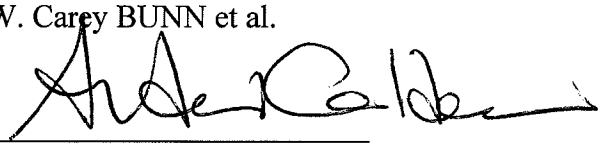
> In order to provide a complete application file history and to enhance the clarity of the prosecution history record, an examiner must provide clear explanations of all actions taken by the examiner during the prosecution of an application. (emphasis added).

Applicants submit that Bunker is a complex document (for example, Bunker includes 23 figures and 213 paragraphs of written description), such that the pertinence of Bunker as it applies to each respective claim feature is not readily apparent. Accordingly, Applicants respectfully request that, should the rejection be maintained, the Examiner specifically identify exactly which elements of Bunker are considered to read on each respective claim feature (e.g., (i) reviewing security of a network perimeter architecture; (ii) reviewing security of data processing devices that transfer data across the perimeter of the network; (iii) reviewing security of applications that transfer data across said perimeter; and (iv) reviewing vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter).

CONCLUSION

In view of the foregoing remarks, Applicants submit that all of the claims are patentably distinct from the prior art of record and are in condition for allowance. The Examiner is respectfully requested to pass the above application to issue. The Examiner is invited to contact the undersigned at the telephone number listed below, if needed. Applicants hereby make a written conditional petition for extension of time, if required. Please charge any deficiencies in fees and credit any overpayment of fees to Attorney's Deposit Account No. 09-0457.

Respectfully submitted,
W. Carey BUNN et al.



Andrew M. Calderon
Registration No. 38,093

November 19, 2007
Greenblum & Bernstein, P.L.C.
1950 Roland Clarke Place
Reston, Virginia 20191
Telephone: 703-716-1191